i.MX8 and i.MX9 SHE API Rev 0.1 NXP Copyright

Generated by Doxygen 1.8.17

1 SHE API	1
2 Revision History	1
3 General concepts related to the API	1
3.1 Session	. 1
4 Module Index	1
4.1 Modules	. 1
5 Module Documentation	2
5.1 CMD_ENC_CBC / CMD_DEC_CBC and CMD_ENC_ECB / CMD_DEC_ECB	. 2
5.1.1 Detailed Description	. 3
5.1.2 Macro Definition Documentation	. 3
5.1.3 Typedef Documentation	. 3
5.1.4 Function Documentation	. 3
5.2 CMD_EXPORT_RAM_KEY	. 5
5.2.1 Detailed Description	. 5
5.2.2 Data Structure Documentation	
5.2.3 Function Documentation	. 5
5.3 FAST MAC	. 7
5.3.1 Detailed Description	
5.3.2 Data Structure Documentation	
5.3.3 Macro Definition Documentation	
5.4 CMD GENERATE MAC	
5.4.1 Detailed Description	
5.4.2 Data Structure Documentation	
5.4.3 Function Documentation	
5.5 CMD VERIFY MAC	
5.5.1 Detailed Description	
5.5.2 Data Structure Documentation	
5.5.3 Function Documentation	
5.6 SHE get info	
5.6.1 Detailed Description	
5.6.2 Function Documentation	
5.7 SHE commands	
5.7.1 Detailed Description	
5.8 CMD_GET_STATUS	
5.8.1 Detailed Description	
5.8.2 Data Structure Documentation	
5.8.3 Function Documentation	
5.9 Session	
5.9.1 Detailed Description	
5.9.2 Data Structure Documentation	. 17

5.9.3 Macro Definition Documentation	18
5.9.4 Typedef Documentation	19
5.9.5 Function Documentation	19
5.10 Key store	22
5.10.1 Detailed Description	22
5.10.2 Data Structure Documentation	23
5.10.3 Macro Definition Documentation	24
5.10.4 Function Documentation	24
5.11 CMD_LOAD_KEY	26
5.11.1 Detailed Description	26
5.11.2 Data Structure Documentation	26
5.11.3 Function Documentation	27
5.12 CMD_LOAD_PLAIN_KEY	29
5.12.1 Detailed Description	29
5.12.2 Data Structure Documentation	29
5.12.3 Function Documentation	29
5.13 CMD_INIT_RNG	30
5.13.1 Detailed Description	30
5.13.2 Function Documentation	30
5.14 CMD_RND	31
5.14.1 Detailed Description	31
5.14.2 Data Structure Documentation	31
5.14.3 Macro Definition Documentation	31
5.14.4 Function Documentation	32
5.15 CMD_EXTEND_SEED	33
5.15.1 Detailed Description	33
5.15.2 Data Structure Documentation	33
5.15.3 Macro Definition Documentation	33
5.15.4 Function Documentation	33
5.16 Shared Buffer	35
5.16.1 Detailed Description	35
5.16.2 Data Structure Documentation	35
5.17 Error codes	37
5.17.1 Detailed Description	37
5.17.2 Enumeration Type Documentation	37
5.18 Utils	39
5.18.1 Detailed Description	39
5.18.2 Data Structure Documentation	39
5.18.3 Function Documentation	39
5.19 last rating code	42
5.19.1 Detailed Description	42
5.19.2 Function Documentation	42

5.2	20 CMD_CANCEL	43
	5.20.1 Detailed Description	43
	5.20.2 Function Documentation	43
5.2	21 Get Info	44
	5.21.1 Detailed Description	44
	5.21.2 Data Structure Documentation	44
5.2	22 Global Info	45
	5.22.1 Detailed Description	46
	5.22.2 Function Documentation	46
Index		51

1 SHE API

This document is a software referece description of the API provided by the i.MX8 SHE solutions.

2 Revision History

Revision	date	description
0.1	Jul 06 2023	first draft

3 General concepts related to the API

3.1 Session

The API must be initialized by a potential requestor by opening a session.

The session establishes a route (MU, DomainID...) between the requester and the SHE module, and grants the usage of a specified key store. When a session is opened, the SHE module returns a handle identifying the session to the requester.

4 Module Index

4.1 Modules

Here is a list of all modules:

SHE get info	14
SHE commands	15
CMD_ENC_CBC / CMD_DEC_CBC and CMD_ENC_ECB / CMD_DEC_ECB	2
CMD_EXPORT_RAM_KEY	5

	FAST_MAC	7
	CMD_GENERATE_MAC	9
	CMD_VERIFY_MAC	11
	CMD_GET_STATUS	16
	CMD_LOAD_KEY	26
	CMD_LOAD_PLAIN_KEY	29
	CMD_INIT_RNG	30
	CMD_RND	31
	CMD_EXTEND_SEED	33
	last rating code	42
	CMD_CANCEL	43
Se	ession	17
Κe	ey store	22
Sł	nared Buffer	35
Er	ror codes	37
Ut	iils	39
G	et Info	44
GI	obal Info	45

5 Module Documentation

5.1 CMD ENC CBC / CMD DEC CBC and CMD ENC ECB / CMD DEC ECB

Macros

- #define SHE_CIPHER_ONE_GO_ALGO_AES_ECB ((she_op_cipher_one_go_algo_t)(0x00u))
- #define SHE_CIPHER_ONE_GO_ALGO_AES_CBC ((she_op_cipher_one_go_algo_t)(0x01u))
- #define SHE_CIPHER_ONE_GO_ALGO_AES_CCM ((she_op_cipher_one_go_algo_t)(0x04u))
- #define SHE_CIPHER_ONE_GO_ALGO_SM4_ECB ((she_op_cipher_one_go_algo_t)(0x10u))
- #define SHE_CIPHER_ONE_GO_ALGO_SM4_CBC ((she_op_cipher_one_go_algo_t)(0x11u))
- #define SHE_CIPHER_ONE_GO_FLAGS_DECRYPT ((she_op_cipher_one_go_flags_t)(0u << 0))
- #define SHE_CIPHER_ONE_GO_FLAGS_ENCRYPT ((she_op_cipher_one_go_flags_t)(1u << 0))

Typedefs

- typedef uint8_t she_op_cipher_one_go_algo_t
- typedef uint8_t she_op_cipher_one_go_flags_t

Functions

- she err t she open cipher service (she hdl t session hdl, open svc cipher args t *args)
- she_err_t she_close_cipher_service (she_hdl_t cipher_handle)
- she_err_t she_cipher_one_go (she_hdl_t cipher_handle, op_cipher_one_go_args_t *args)

5.1.1 Detailed Description

5.1.2 Macro Definition Documentation

5.1.2.1 SHE_CIPHER_ONE_GO_ALGO_AES_CCM #define SHE_CIPHER_ONE_GO_ALGO_AES_CCM ((she_op_cipher_one_go_algo_aes_ccm ((she_op_cipher_one_go_aes_ccm (she_op_cipher_one_go_aes_ccm (she_op_cip

• AES CCM where: - Adata = 0, - Tlen = 16 bytes, - nonce size = 12 bytes

```
5.1.2.2 SHE_CIPHER_ONE_GO_FLAGS_DECRYPT #define SHE_CIPHER_ONE_GO_FLAGS_DECRYPT ((she_op_cipher_one_go << 0))
```

Bit indicating the decrypt operation

```
5.1.2.3 SHE_CIPHER_ONE_GO_FLAGS_ENCRYPT #define SHE_CIPHER_ONE_GO_FLAGS_ENCRYPT ((she_op_cipher_one_go << 0))
```

Bit indicating the encrypt operation

5.1.3 Typedef Documentation

```
5.1.3.1 she op cipher one go algo t typedef uint8_t she_op_cipher_one_go_algo_t
```

Bit field indicating the requested cipher operations

```
5.1.3.2 she_op_cipher_one_go_flags_t typedef uint8_t she_op_cipher_one_go_flags_t
```

Bit field indicating the requested encrypt/decrypt operations

5.1.4 Function Documentation

- · Open a cipher service flow.
- · User can call this function only after having opened a key-store service flow.
- User must open this service in order to perform cipher operation.

Parameters

session_hdl	handle identifying the SHE session.
args	pointer to the structure containing the function arguments.

Returns

error code.

5.1.4.2 she_close_cipher_service() she_err_t she_close_cipher_service (she_hdl_t $cipher_handle$)

Terminate a previously opened cipher service flow

Parameters

	cipher_handle	handle identifying the Cipher service.
--	---------------	--

Returns

error code.

Perform ciphering operation i.e.

CBC encryption/decryption and ECB encryption/decryption of a given plaintext/ciphertext with the key identified by key_id.

User can call this function only after having opened a cipher service flow

Parameters

session_hdl	handle identifying the SHE session.
args	pointer to the structure containing the function arguments.

Returns

5.2 CMD_EXPORT_RAM_KEY

Data Structures

• struct op_export_plain_key_args_t

Functions

she_err_t she_export_plain_key (she_hdl_t utils_handle, op_export_plain_key_args_t *args)

5.2.1 Detailed Description

5.2.2 Data Structure Documentation

5.2.2.1 struct op_export_plain_key_args_t Structure describing the export RAM key operation arguments

Data Fields

uint8_t *	m1	< identifier of the key to be used for the operation pointer to the output address for M1 message
uint8_t	m1_size	size of M1 message - 128 bits
uint8_t *	m2	pointer to the output address for M2 message
uint8_t	m2_size	size of M2 message - 256 bits
uint8_t *	m3	pointer to the output address for M3 message
uint8_t	m3_size	size of M3 message - 128 bits
uint8_t *	m4	pointer to the output address for M4 message
uint8_t	m4_size	size of M4 message - 256 bits
uint8_t *	m5	pointer to the output address for M5 message
uint8_t	m5_size	size of M5 message - 128 bits

5.2.3 Function Documentation

exports the RAM_KEY into a format protected by SECRET_KEY.

Parameters

utils_handle	handle identifying the SHE utils service.
args	pointer to the structure containing the function arguments.

Returns

5.3 FAST_MAC 7

5.3 FAST_MAC

Data Structures

- struct op_fast_seco_mac_t
- struct op_fast_v2x_mac_t

Macros

- #define SHE_FAST_MAC_FLAGS_GENERATION 0
- #define SHE_FAST_MAC_FLAGS_VERIFICATION 1
- #define SHE_FAST_MAC_FLAGS_VERIF_BIT_LEN 2

5.3.1 Detailed Description

5.3.2 Data Structure Documentation

5.3.2.1 struct op_fast_seco_mac_t Structure describing the fast mac generation operation arguments for $S \leftarrow ECO$

Data Fields

uint16_t	key_id	identifier of the key to be used for the operation
uint16_t	data_length	length in bytes of the input message. The message is padded to be a multiple of 128 bits by SHE
uint16_t	data_offset	Offset of the Input data in the SECURE RAM.
uint8_t	mac_length	MAC length in bytes, only valid in case of MAC verification.
uint8_t	flags	flag to identify the operation(generate/verify)
uint32_t	verification_status	result of the MAC comparison

5.3.2.2 struct op_fast_v2x_mac_t Structure describing the fast mac generation operation arguments for V2X

Data Fields

uint16_t	key_id	identifier of the key to be used for the operation
uint16_t	data_length	length in bytes of the input message. The message is padded to be a multiple of 128 bits by SHE
uint16_t	rsrv	reserved
uint8_t	mac_length	MAC length expressed in bits, only valid in case of MAC verification. Accepted values are: Zero: the MAC length value used will be the nominal length (128bit). Greater or equal than the minimum value defined in the key store.
uint8_t	flags	flag to identify the operation(generate/verify)
uint32_t	m1	
uint32_t	m2	
uint32_t	m3	
uint32_t	m4	The message to use for MAC generation or verification.
uint32_t	verification_status	result of the MAC comparison

5.3.3 Macro Definition Documentation

5.3.3.1 SHE_FAST_MAC_FLAGS_GENERATION #define SHE_FAST_MAC_FLAGS_GENERATION 0

Macros to identify MAC operation type

5.4 CMD_GENERATE_MAC

Data Structures

- struct op_generate_mac_t
- struct op_get_id_args_t

Macros

- #define SHE_MAC_SIZE 16u
 - size of the MAC generated is 128bits.
- #define SHE_CHALLENGE_SIZE 16u /* 128 bits */

size of the input challenge vector is 128 bits.

- #define SHE_ID_SIZE 15u /* 120 bits */
 - size of the Identity(ID) returned is 120 bits.
- #define SHE_MAC_SIZE 16u /* 128 bits */

size of the computed MAC is 128 bits.

Functions

- she_err_t she_generate_mac (she_hdl_t utils_handle, op_generate_mac_t *args)
- she_err_t she_get_id (she_hdl_t utils_handle, op_get_id_args_t *args)

5.4.1 Detailed Description

5.4.2 Data Structure Documentation

5.4.2.1 struct op_generate_mac_t Structure describing the fast mac generation operation arguments

Data Fields

uint16_t	key_ext	identifier of the key extension to be used for the operation	
uint16_t	key_id	identifier of the key to be used for the operation	
uint16_t	message_length	length in bytes of the input message. The message is padded to be a multiple of 128 bits by SHE	
uint8_t *	message	pointer to the message to be processed	
uint8_t *	mac	pointer to where the output MAC should be written (128bits should be allocated there)	

5.4.2.2 struct op_get_id_args_t Structure describing the fast mac generation operation arguments for SECO

Data Fields

uint8_t	challenge[SHE_CHALLENGE_SIZE]	Challenge vector.
uint8_t	id[SHE_ID_SIZE]	identity (UID) returned by the command
uint8_t	sreg	status register returned by the command
uint8_t	mac[SHE_MAC_SIZE]	MAC returned by the command.

5.4.3 Function Documentation

Generates a MAC of a given message with the help of a key identified by key_id.

Parameters

utils_handle	handle identifying the utils service.
args	pointer to the structure containing the function arguments.

Returns

error code

This function returns the identity (UID) and the value of the status register protected by a MAC over a challenge and the data. User can call this function only after getting the utility service.

Parameters

utils_handle	handle identifying the utils service.
args	pointer to the structure containing the function arguments.

Returns

5.5 CMD_VERIFY_MAC

Data Structures

struct op_verify_mac_t

Macros

- #define SHE_FAST_MAC_VERIFICATION_STATUS_OK 0x5a3cc3a5
- #define MAC_BYTES_LENGTH 0
- #define MAC_BITS_LENGTH 1
- #define SHE_MAC_VERIFICATION_SUCCESS 0

indication of mac verification success

#define SHE_MAC_VERIFICATION_FAILED 1

indication of mac verification failure

Functions

• she_err_t she_verify_mac (she_hdl_t utils_handle, op_verify_mac_t *args)

5.5.1 Detailed Description

5.5.2 Data Structure Documentation

5.5.2.1 struct op_verify_mac_t Structure describing the fast mac generation operation arguments

Data Fields

uint16_t	key_ext	identifier of the key extension to be used for the operation	
uint16_t	key_id	identifier of the key to be used for the operation	
uint16_t	message_length	length in bytes of the input message. The message is padded to be a multiple of 128 bits by SHE	
uint8_t *	message	pointer to the message to be processed	
uint8_t *	mac	pointer to the MAC to be compared	
uint8_t	mac_length	number of MAC bytes to be compared with the expected value. It cannot be lower than 4 bytes.	
uint32_t	verification_status	result of the MAC comparison	
uint8_t	mac_length_encoding		

5.5.3 Function Documentation

Verify the MAC of a given message with the help of a key identified by key_id.

Parameters

utils_handle	handle identifying the utils service.
args	pointer to the structure containing the function arguments.

Returns

5.6 SHE get info

Functions

```
• she_err_t she_get_info (she_hdl_t session_hdl, op_get_info_args_t *args)
```

5.6.1 Detailed Description

5.6.2 Function Documentation

Perform device attestation operation Get miscellaneous information. This function return, among others, all the information needed to build a valid signed message. User can call this function only after having opened the session.

Parameters

sess_hdl	handle identifying the active session.
args	pointer to the structure containing the function arguments.

Returns

5.7 SHE commands 15

5.7 SHE commands

Modules

- CMD_ENC_CBC / CMD_DEC_CBC and CMD_ENC_ECB / CMD_DEC_ECB
- CMD_EXPORT_RAM_KEY
- FAST_MAC
- CMD_GENERATE_MAC
- CMD_VERIFY_MAC
- CMD_GET_STATUS
- CMD_LOAD_KEY
- CMD_LOAD_PLAIN_KEY
- CMD_INIT_RNG
- CMD_RND
- CMD_EXTEND_SEED
- · last rating code
- CMD_CANCEL

5.7.1 Detailed Description

5.8 CMD_GET_STATUS

Data Structures

• struct op_get_status_args_t

Functions

• she_err_t she_get_status (she_hdl_t utils_handle, op_get_status_args_t *args)

5.8.1 Detailed Description

5.8.2 Data Structure Documentation

5.8.2.1 struct op_get_status_args_t Structure describing the get status operation arguments

Data Fields

uint8_t	sreg	status register bits	
uint8_t	pad[3]	padding bytes	

5.8.3 Function Documentation

Command to get the content of the status register

Parameters

session_hdl	handle identifying the utils service
args	pointer to the structure containing the function arguments.

Returns

5.9 Session 17

5.9 Session

Data Structures

- · struct she session hdl s
- struct she_service_hdl_s
- · struct open_session_args_t

Macros

- #define SHE HANDLE NONE (0x0)
- #define SHE_MAX_SESSIONS (8u)

Maximum sessions supported.

• #define SHE_MAX_SERVICES (32u)

Maximum services supported.

#define MAX_KEY_STORE_SESSIONS (5u)

Maximum Key store sessions supported.

- #define SHE_OPEN_SESSION_PRIORITY_LOW (0x00U)
- #define SHE OPEN SESSION PRIORITY HIGH (0x01U)
- #define SHE OPEN SESSION FIPS MODE MASK BIT(0)
- #define SHE_OPEN_SESSION_EXCLUSIVE_MASK BIT(1)
- #define SHE OPEN SESSION LOW LATENCY MASK BIT(3)
- #define SHE_OPEN_SESSION_NO_KEY_STORE_MASK BIT(4)

Typedefs

• typedef uint32_t she_hdl_t

Functions

- struct she_session_hdl_s * she_session_hdl_to_ptr (uint32_t hdl)
- void delete_she_session (struct she_session_hdl_s *s_ptr)
- struct she_session_hdl_s * add_she_session (void)
- struct she_service_hdl_s * she_service_hdl_to_ptr (uint32_t hdl)
- void delete_she_service (struct she_service_hdl_s *s_ptr)
- struct she_service_hdl_s * add_she_service (struct she_session_hdl_s *session)
- she_err_t she_open_session (open_session_args_t *args, she_hdl_t *session_hdl)
- she_err_t she_close_session (she_hdl_t session_hdl)

5.9.1 Detailed Description

5.9.2 Data Structure Documentation

5.9.2.1 struct she_session_hdl_s Structure describing the session handle members

Data Fields

struct plat_os_abs_hdl	* phdl	Pointer to OS device node.
uint32	t session_hd	Session handle.
uint32	_t mu_type	Session MU type.
Generated by Doxygen uint32	t last_rating	last error code returned by command.

5.9.2.2 struct she_service_hdl_s Structure describing the service handle members

Data Fields

struct she_session_hdl_s *	session	Pointer to session handle.
uint32_t	service_hdl	Service handle.

5.9.2.3 struct open_session_args_t Structure detailing the open session operation member arguments

Data Fields

uint32_t	session_hdl	Session handle.
uint32_t	mu_type	MU type on which session will be opened.
uint8_t	session_priority	Priority of the operations performed in this session.
uint8_t	operating_mode	Options for the session to be opened (bitfield).
uint8_t	interrupt_idx	Interrupt number of the MU used to indicate data availability.
uint8_t	mu_id	index of the MU as per PLAT point of view.
uint8_t	tz	indicate if current partition has TZ enabled.
uint8_t	did	DID of the calling partition.

5.9.3 Macro Definition Documentation

5.9.3.1 SHE_HANDLE_NONE #define SHE_HANDLE_NONE (0x0)

Handle not available

5.9.3.2 SHE_OPEN_SESSION_PRIORITY_LOW #define SHE_OPEN_SESSION_PRIORITY_LOW (0x00U)

Session opening priority flags Low priority. default setting on platforms that doesn't support sessions priorities.

5.9.3.3 SHE_OPEN_SESSION_PRIORITY_HIGH #define SHE_OPEN_SESSION_PRIORITY_HIGH (0x01U) High Priority session.

5.9.3.4 SHE_OPEN_SESSION_FIPS_MODE_MASK #define SHE_OPEN_SESSION_FIPS_MODE_MASK BIT(0)

5.9.3.5 SHE_OPEN_SESSION_EXCLUSIVE_MASK #define SHE_OPEN_SESSION_EXCLUSIVE_MASK BIT(1)

No other SHE session will be authorized on the same security enclave.

Operating Mode Only FIPS certified operations authorized in this session.

5.9 Session 19

```
5.9.3.6 SHE_OPEN_SESSION_LOW_LATENCY_MASK #define SHE_OPEN_SESSION_LOW_LATENCY_MA↔ SK BIT(3)
```

Use a low latency SHE implementation.

```
5.9.3.7 SHE_OPEN_SESSION_NO_KEY_STORE_MASK #define SHE_OPEN_SESSION_NO_KEY_STORE_MA↔ SK BIT(4)
```

No key store will be attached to this session. May provide better performances on some operation depending on the implementation. Usage of the session will be restricted to operations that doesn't involve secret keys (e.g. hash, signature verification, random generation)

5.9.4 Typedef Documentation

```
5.9.4.1 she_hdl_t typedef uint32_t she_hdl_t
```

Define the SHE handle type

5.9.5 Function Documentation

```
5.9.5.1 she_session_hdl_to_ptr() struct she_session_hdl_s* she_session_hdl_to_ptr ( uint32_t hdl )
```

Returns pointer to the session handle

Parameters

hdl identifying the session handle.

Returns

pointer to the session handle.

Delete the session

Parameters

s_ptr pointer identifying the session.

```
5.9.5.3 add_she_session() struct she_session_hdl_s* add_she_session ( void )
```

Add the session

Returns

pointer to the session.

```
5.9.5.4 she_service_hdl_to_ptr() struct she_service_hdl_s* she_service_hdl_to_ptr ( uint32_t hdl)
```

Returns pointer to the service handle

Parameters

hdl identifying the session handle.

Returns

pointer to the service handle.

```
5.9.5.5 delete_she_service() void delete_she_service ( struct she_service_hdl_s * s_ptr )
```

Delete the service

Parameters

s_ptr pointer identifying the service.

5.9 Session 21

Add the service

Returns

pointer to the service.

Parameters

args	pointer to the structure containing the function arguments.
session_hdl	pointer to where the session handle must be written.

Returns

error code.

Terminate a previously opened session. All the services opened under this session are closed as well

Parameters

session_hdl	pointer to the handle identifying the session to be closed.
-------------	---

Returns

5.10 Key store

User must open a key store service flow in order to perform the following operations:

Data Structures

- · struct open_svc_key_store_args_t
- struct op_key_store_reprov_en_args_t

Macros

- #define KEY STORE OPEN FLAGS DEFAULT 0x0u
- #define KEY_STORE_OPEN_FLAGS_CREATE 0x1u
- #define KEY_STORE_OPEN_FLAGS_SHE 0x2u
- #define KEY STORE OPEN FLAGS SET MAC LEN 0x8u
- #define KEY_STORE_OPEN_FLAGS_SHARED 0x20u
- #define KEY STORE OPEN FLAGS STRICT OPERATION 0x80u
- #define SHE STORAGE NUMBER UPDATES DEFAULT 300u
- #define SHE_STORAGE_MIN_MAC_BIT_LENGTH_DEFAULT 32u

Functions

- she_err_t she_open_key_store_service (she_hdl_t session_hdl, open_svc_key_store_args_t *args)
- she_err_t she_close_key_store_service (she_hdl_t key_store_handle)

5.10.1 Detailed Description

User must open a key store service flow in order to perform the following operations:

- · create a new key store
- perform operations involving keys stored in the key store (ciphering, signature generation...)
- perform a key store reprovisioning using a signed message. A key store re-provisioning results in erasing all the key stores handled by the SHE.

To grant access to the key store, the caller is authenticated against the domain ID (DID) and Messaging Unit used at the keystore creation, additionally an authentication nonce can be provided.

5.10 Key store 23

Data Fields

5.10.2 Data Structure Documentation

5.10.2.1 struct open_svc_key_store_args_t Structure specifying the open key store service member arguments

Data Fields

uint32_t	key_store_hdl	handle identifying the key store service flow
uint32_t	key_store_identifier	user defined id identifying the key store. Only one key store service can be opened on a given key_store_identifier.
uint32_t	authentication_nonce	user defined nonce used as authentication proof for accessing the key store.
uint8_t	flags	bitmap specifying the services properties.
uint16_t	max_updates_number	maximum number of updates authorized for the key store.
		Valid only for create operation.
		This parameter has the goal to limit the occupation of the monotonic counter used as anti-rollback protection.
		 If the maximum number of updates is reached, HSM still allows key store updates but without updating the monotonic counter giving the opportunity for rollback attacks.
uint8_t	min_mac_length	it corresponds to the minimum mac length (in bits) accepted to perform MAC verification operations. Only used upon key store creation when KEY_STORE_FLAGS_SET_MAC_LEN bit is set. It is effective only for MAC verification operations with the mac length expressed in bits. It can be used to replace the default value (32 bits). It impacts all MAC algorithms and all key lengths. It must be different from 0. When in FIPS approved mode values < 32 bits are not allowed. Only used on devices implementing SECO FW.
uint8_t *	signed_message	pointer to signed_message to be sent only in case of key store re-provisioning.
uint16_t	signed_msg_size	size of the signed_message to be sent only in case of key store re-provisioning.

$\textbf{5.10.2.2} \quad \textbf{struct op_key_store_reprov_en_args_t} \quad \text{Structure describing the key store reprovisioning enable operation arguments}$

Data Fields

uint8_t *	signed_message	signed content payload
uint32_t	signed_msg_size	signed content payload size in bytes

5.10.3 Macro Definition Documentation

5.10.3.1 KEY_STORE_OPEN_FLAGS_DEFAULT #define KEY_STORE_OPEN_FLAGS_DEFAULT 0x0u default flags

5.10.3.2 KEY_STORE_OPEN_FLAGS_CREATE #define KEY_STORE_OPEN_FLAGS_CREATE 0x1u Create a key store

5.10.3.3 KEY_STORE_OPEN_FLAGS_SHE #define KEY_STORE_OPEN_FLAGS_SHE 0x2u

Target key store is a SHE key store

5.10.3.4 KEY_STORE_OPEN_FLAGS_SET_MAC_LEN #define KEY_STORE_OPEN_FLAGS_SET_MAC_L↔ EN 0x8u

Check min mac length

5.10.3.5 KEY_STORE_OPEN_FLAGS_SHARED #define KEY_STORE_OPEN_FLAGS_SHARED 0x20u

Target key store is a shared key store

5.10.3.6 KEY_STORE_OPEN_FLAGS_STRICT_OPERATION #define KEY_STORE_OPEN_FLAGS_STRICT_O↔ PERATION 0x80u

The request is completed only when the key store has been written in the NVM and the monotonic counter has been updated. This flag is applicable for CREATE operation only

 $\textbf{5.10.3.7} \quad \textbf{SHE_STORAGE_NUMBER_UPDATES_DEFAULT} \quad \texttt{\#define} \quad \texttt{SHE_STORAGE_NUMBER_UPDATES_DEFAU} \leftarrow \\ \texttt{LT 300u} \quad \texttt{} \\$

default number of maximum number of updated for SHE storage.

 $\textbf{5.10.3.8} \quad \textbf{SHE_STORAGE_MIN_MAC_BIT_LENGTH_DEFAULT} \quad \texttt{\#define SHE_STORAGE_MIN_MAC_BIT_LENG} \\ \text{TH_DEFAULT } \quad \texttt{32u} \\$

default MAC verification length in bits

5.10.4 Function Documentation

Open a service flow on the specified key store.

5.10 Key store 25

Parameters

session_hdl	SHE handle identifying the current session.
args	pointer to the structure containing the function arguments.

Returns

error code.

$$\textbf{5.10.4.2} \quad \textbf{she_close_key_store_service()} \quad \textbf{she_err_t} \quad \textbf{she_close_key_store_service (} \\ \quad \textbf{she_hdl_t} \quad \textit{key_store_handle} \)$$

Terminate a previously opened key store service flow

Parameters

key_store_handle	handle identifying the key store service.
------------------	---

Returns

5.11 CMD_LOAD_KEY

Data Structures

- struct op_key_update_args_t
- struct op_key_update_ext_args_t

Macros

• #define SHE_LOAD_KEY_EXT_FLAGS_STRICT_OPERATION BIT(7)

Functions

- she_err_t she_key_update (she_hdl_t utils_handle, op_key_update_args_t *args)
- she_err_t she_key_update_ext (she_hdl_t utils_handle, op_key_update_ext_args_t *args)

5.11.1 Detailed Description

5.11.2 Data Structure Documentation

5.11.2.1 struct op_key_update_args_t Structure describing the key update operation arguments

Data Fields

utils_handle	Handle to utils service.
key_ext	identifier of the key extension to be used for the operation
key_id	identifier of the key to be used for the operation
m1	pointer to M1 message
m1_size	size of M1 message - 128 bits
m2	pointer to M2 message
m2_size	size of M2 message - 256 bits
m3	pointer to M3 message
m3_size	size of M3 message - 128 bits
m4	pointer to the output address for M4 message
m4_size	size of M4 message - 256 bits
m5	pointer to the output address for M5 message
m5_size	size of M5 message - 128 bits
	key_ext key_id m1 m1_size m2 m2_size m3 m3_size m4 m4_size m5

5.11.2.2 struct op_key_update_ext_args_t Structure describing the key update extension operation arguments

Data Fields

uint32_t	utils_handle	Handle to utils service.
uint32_t	key_ext	identifier of the key extension to be used for the operation
uint32_t	key_id	identifier of the key to be used for the operation
uint8_t *	m1	pointer to M1 message

Data Fields

uint8_t	m1_size	size of M1 message - 128 bits
uint8_t *	m2	pointer to M2 message
uint8_t	m2_size	size of M2 message - 256 bits
uint8_t *	m3	pointer to M3 message
uint8_t	m3_size	size of M3 message - 128 bits
uint8_t *	m4	pointer to the output address for M4 message
uint8_t	m4_size	size of M4 message - 256 bits
uint8_t *	m5	pointer to the output address for M5 message
uint8_t	m5_size	size of M5 message - 128 bits
uint8_t	flags	bitmap specifying the operations property

5.11.3 Function Documentation

Update an internal key of SHE with the protocol specified by SHE. The request is completed only when the new key has been written in the NVM. The monotonic counter is incremented for each successful update.

Parameters

utils_handle	handle identifying the utils service.
args	pointer to the structure containing the function arguments.

Returns

error code

This is an extension of the CMD_LOAD_KEY The functionality of the CMD_LOAD_KEY is extended by adding a flag argument The updates to the key store must be considered as effective only after an operation specifying the flag "STRICT OPERATION" is aknowledged by SHE

The request is completed only when the key store is written in the NVM and the monotonic counter is incremented

Parameters

utils_handle	handle identifying the utils service
args	pointer to the structure containing the function arguments.

Returns

5.12 CMD_LOAD_PLAIN_KEY

Data Structures

struct op_load_plain_key_args_t

Functions

• she_err_t she_load_plain_key (she_hdl_t utils_handle, op_load_plain_key_args_t *args)

5.12.1 Detailed Description

5.12.2 Data Structure Documentation

5.12.2.1 struct op_load_plain_key_args_t Structure describing the plain key load operation arguments

Data Fields

```
uint8_t key[SHE_KEY_SIZE_IN_BYTES] pointer to plain key
```

5.12.3 Function Documentation

Load a key as plaintext to the RAM_KEY slot without encryption and verification.

Parameters

hdl	pointer to the SHE utils handle
key	pointer to the plaintext key to be loaded - 128bits

Returns

5.13 CMD_INIT_RNG

Functions

- she_err_t she_open_rng_service (she_hdl_t session_hdl, open_svc_rng_args_t *args)
- she_err_t she_close_rng_service (she_hdl_t rng_handle)

5.13.1 Detailed Description

5.13.2 Function Documentation

initializes the seed and derives a key for the PRNG. The function must be called before CMD_RND after every power cycle/reset.

User can call this function only after having opened a session.

Parameters

session_hdl	handle identifying the current session.
args	pointer to the structure containing the function arguments.

Returns

error code

Terminate a previously opened rng service flow

Parameters

Returns

5.14 CMD RND 31

5.14 CMD_RND

Data Structures

- struct open_svc_rng_args_t
- struct op_get_random_args_t

Macros

• #define SHE_RND_SIZE 16u

Typedefs

typedef uint8_t svc_rng_flags_t

Functions

• she_err_t she_get_random (she_hdl_t rng_handle, op_get_random_args_t *args)

5.14.1 Detailed Description

5.14.2 Data Structure Documentation

Data Fields

svc_rng_flags_t	flags	bitmap indicating the service flow properties
uint8_t	reserved[3]	
uint32_t	rng_hdl	rng handle

5.14.2.1 struct open_svc_rng_args_t

5.14.2.2 struct op_get_random_args_t Structure detailing the get random number operation member arguments

Data Fields

uint8_t *	output	pointer to the output area where the random number must be written
uint32_t	random_size	length in bytes of the random number to be provided.
svc_rng_flags_t	svc_flags	bitmap indicating the service flow properties
uint8_t	reserved[3]	

5.14.3 Macro Definition Documentation

5.14.3.1 SHE_RND_SIZE #define SHE_RND_SIZE 16u

size of random data for SHE

5.14.4 Function Documentation

returns a vector of 128 random bits. The random number generator has to be initialized by CMD_INIT_RNG before random numbers can be supplied.

Parameters

rng_handle	handle identifying the RNG service	
args	pointer to the structure containing the function arguments.	

Returns

5.15 CMD_EXTEND_SEED

Data Structures

· struct op_rng_extend_seed_t

Macros

• #define SHE_ENTROPY_SIZE 16u

Functions

• she_err_t she_extend_seed (she_hdl_t rng_handle, op_rng_extend_seed_t *args)

5.15.1 Detailed Description

5.15.2 Data Structure Documentation

5.15.2.1 struct op_rng_extend_seed_t Structure describing the RNG extend seed operation arguments

Data Fields

uint32_t	entropy[4]	< entropy to extend seed entropy size
uint32_t	entropy_size	

5.15.3 Macro Definition Documentation

```
5.15.3.1 SHE_ENTROPY_SIZE #define SHE_ENTROPY_SIZE 16u
```

size of entropy for SHE

5.15.4 Function Documentation

extends the seed of the PRNG by compressing the former seed value and the supplied entropy into a new seed which will be used to generate the following random numbers. The random number generator has to be initialized by CMD_INIT_RNG before the seed can be extended.

Parameters

rng_handle	handle identifying the RNG service
args	pointer to the structure containing entropy vector (128bits)

Returns

error code

5.16 Shared Buffer 35

5.16 Shared Buffer

Data Structures

- struct op_shared_buf_args_t
- struct open_svc_cipher_args_t
- struct op_cipher_one_go_args_t

5.16.1 Detailed Description

5.16.2 Data Structure Documentation

5.16.2.1 struct op_shared_buf_args_t Structure describing the get shared buffer operation arguments

Data Fields

uint16_t	shared_buf_offset	offset of the shared buffer in secure memory
uint16_t	shared_buf_size	size in bytes of the allocated shared buffer

5.16.2.2 struct open_svc_cipher_args_t Structure describing the open cipher service members

Data Fields

uint32_t	cipher_hdl	handle identifying the cipher service flow
uint8_t	flags	bitmap specifying the services properties
uint8_t	reserved[3]	

$\textbf{5.16.2.3} \quad \textbf{struct op_cipher_one_go_args_t} \quad \text{Structure describing the cipher one go operation arguments}$

Data Fields

uint32_t	key_identifier	identifier of the key to be used for the operation	
uint8_t *	iv	pointer to the initialization vector (nonce in case of AES CCM)	
uint16_t	iv_size	length in bytes of the initialization vector. it must be 0 for algorithms not using the initialization vector. It must be 12 for AES in CCM mode	
uint8_t	svc_flags	bitmap specifying the services properties.	
uint8_t	flags	bitmap specifying the operation attributes	
uint8_t	cipher_algo	algorithm to be used for the operation	
uint8_t *	input	pointer to the input area: • plaintext for encryption	
uint8_t *	output	 ciphertext for decryption Note: In case of CCM it is the purported ciphertext. pointer to the output area: ciphertext for encryption Note: In case of CCM it is the output of the generation-encryption process. plaintext for decryption 	

Data Fields

ui	int32_t	input_size	length in bytes of the input.
			 In case of CBC and ECB, the input size should be multiple of a block cipher size (16 bytes).
ui	int32_t	output_size	length in bytes of the output

5.17 Error codes 37

5.17 Error codes

Error codes returned by SHE functions.

Enumerations

```
enum she_err_t {
 SHE_NO_ERROR = 0x00,
 SHE_INVALID_MESSAGE = SAB_INVALID_MESSAGE,
 SHE_INVALID_ADDRESS = SAB_INVALID_ADDRESS,
 SHE UNKNOWN ID = SAB UNKNOWN ID,
 SHE INVALID PARAM = SAB INVALID PARAM,
 SHE NVM ERRO = SAB NVM ERROR,
 SHE_OUT_OF_MEMORY = SAB_OUT_OF_MEMORY,
 SHE UNKNOWN HANDLE = SAB UNKNOWN HANDLE,
 SHE UNKNOWN KEY STORE = SAB UNKNOWN KEY STORE,
 SHE_KEY_STORE_AUTH = SAB_KEY_STORE_AUTH,
 SHE_KEY_STORAGE_ERROR = SAB_KEY_STORAGE_ERROR,
 SHE ID CONFLICT = SAB ID CONFLICT,
 SHE RNG NOT STARTED = SAB RNG NOT STARTED,
 SHE CMD NOT_SUPPORTED = SAB_CMD_NOT_SUPPORTED,
 SHE_INVALID_LIFECYCLE = SAB_INVALID_LIFECYCLE,
 SHE_KEY_STORE_CONFLICT = SAB_KEY_STORE_CONFLICT,
 SHE KEY STORE COUNTER = SAB KEY STORE COUNTER,
 SHE_FEATURE_NOT_SUPPORTED = SAB_FEATURE_NOT_SUPPORTED,
 SHE_SELF_TEST_FAILURE = SAB_SELF_TEST_FAILURE,
 SHE_NOT_READY = SAB_NOT_READY,
 SHE FEATURE DISABLED = SAB FEATURE DISABLED,
 SHE_UNKNOWN_WARNING = 0x27,
 SHE_SEQUENCE_ERROR_RATING = 0xD1,
 SHE_KEY_NOT_AVAILABLE_RATING = 0xD2,
 SHE_KEY_INVALID_RATING = 0xD3,
 SHE_KEY_EMPTY_RATING = 0xD4,
 SHE NO SECURE BOOT RATING = 0xD5,
 SHE KEY WRITE PROTECTED RATING = 0xD6,
 SHE KEY UPDATE ERROR RATING = 0xD7,
 SHE_RNG_SEED_RATING = 0xD8,
 SHE_NO_DEBUGGING_RATING = 0xD9,
 SHE_BUSY_RATING = 0xDA,
 SHE_MEMORY_FAILURE_RATING = 0xDB,
 SHE_GENERAL_ERROR = 0xDC,
 SHE\_LIB\_ERROR = 0xEF,
 SHE FATAL FAILURE = SAB FATAL FAILURE }
```

5.17.1 Detailed Description

Error codes returned by SHE functions.

5.17.2 Enumeration Type Documentation

5.17.2.1 she_err_t enum she_err_t

Error codes returned by SHE functions.

Enumerator

SHE_NO_ERROR SHE_INVALID_MESSAGE Invalid JADDRESS Invalid JAddress. SHE_UNKNOWN_ID Unknown Id. SHE_INVALID_PARAM MU sanity check failed / Invalid parameters. NVM general error. SHE_OUT_OF_MEMORY Internal memory allocation failed. SHE_UNKNOWN_HANDLE SHE_UNKNOWN_HANDLE SHE_UNKNOWN_KEY_STORE Key store with provided key store ID does not exist (load operation). SHE_KEY_STORE_AUTH SHE_KEY_STORE_AUTH SHE_KEY_STORE_AUTH SHE_KEY_STORE_AUTH A key store authentication is failing. SHE_KEY_STORAGE_ERROR Key store vith provided key store ID does not exist (load operation). SHE_KEY_STORAGE_ERROR Key store using the same key id already exists (create operation). SHE_NOT_STARTED Internal RNG not started. SHE_OMD_NOT_SUPPORTED Functionality not supported on current service configuration. SHE_KEY_STORE_CONFELICT SHE_KEY_STORE_CONFELICT SHE_KEY_STORE_CONFELICT SHE_KEY_STORE_CONFELICT SHE_SELF_TEST_FAILURE SHE_SELF_TEST_FAILURE SHE_SELF_TEST_FAILURE SHE_SELF_TEST_FAILURE SHE_SELF_TEST_FAILURE SHE_SELF_TEST_FAILURE SHE_SELF_TEST_FAILURE SHE_SELF_TEST_FAILURE SHE_SELF_TEST_FAILURE SHE_SEQUENCE_ERROR_RATING SHE_KEY_NOT_AVAILABLE_RATING SHE_KEY_NOT_AVAILABLE_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_MS_SELE_TEST_FAILURE SHE_BOST_RATING SHE_BUSY_RATING SHE_BUSY_RA		
SHE_INVALID_ADDRESS SHE_UNKNOWN_ID Unknown Id. SHE_INVALID_PARAM MU sanity check failed / Invalid parameters. SHE_NVM_ERRO NVM general error. Internal memory allocation failed. SHE_UNKNOWN_HANDLE SHE_UNKNOWN_KEY_STORE SHE_UNKNOWN_KEY_STORE SHE_KEY_STORE AUTH A key store authentication is failing. SHE_KEY_STORE_ALTH A key store verith provided key store ID does not exist (load operation). SHE_KEY_STORAGE_ERROR Key store verith provided key store ID does not exist (load operation). SHE_KEY_STORAGE_ERROR Key store creation/load failure. A key store using the same key id already exists (create operation). SHE_RNG_NOT_STARTED Internal RNG not started. SHE_OMD_NOT_SUPPORTED Functionality not supported on current service configuration. SHE_KEY_STORE_CONTLICT The key store already exists (load operation). SHE_KEY_STORE_CONTER SHE_KEY_STORE_COUNTER SHE_KEY_STORE_COUNTER SHE_FEATURE_NOT_SUPPORTED Feature is not supported. SHE_SELF_TEST_FAILURE SHE_NOT_READY System not ready to accept service request. SHE_SHE_FEATURE_DISABLED SHE_UNKNOWN_WARNING SHE_SEQUENCE_ERROR_RATING Invalid sequence of commands. SHE_KEY_INVALID_RATING SHE_KEY_INVALID_RATING SHE_KEY_INVALID_RATING SHE_KEY_INVALID_RATING SHE_KEY_EMPTY_RATING Key has not been initialized yet. SHE_KEY_EMPTY_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_ERROR_SHE MEMORY_FAILURE_RATING SHE_KEY_UPDATE_ERROR_SHE MEMORY_FAILURE_RATING SHE_KEY_UPDATE_ERROR_SHE MEMORY_FAILURE_RATING SHE_KEY_UPDATE_ERROR_SHE M	SHE_NO_ERROR	Success.
SHE_UNKNOWN_ID SHE_INVALID_PARAM MU sanity check failed / Invalid parameters. SHE_NVM_ERRO NVM_general error. Internal memory allocation failed. SHE_UNKNOWN_HANDLE Whoney Handle. SHE_UNKNOWN_KEY_STORE SHE_UNKNOWN_KEY_STORE SHE_KEY_STOREAUTH SHE_KEY_STORAGE_ERROR SHE_ID_CONFLICT SHE_KEY_STORAGE_ERROR SHE_ID_CONFLICT SHE_RNG_NOT_STARTED Internal RNG not started. SHE_KOMD_NOT_STARTED Invalid lifecycle for requested operation). SHE_KEY_STORE_COUNTER SHE_KEY_STORE_COUNTER SHE_KEY_STORE_COUNTER SHE_KEY_STORE_COUNTER SHE_KEY_STORE_COUNTER SHE_FEATURE_NOT_SUPPORTED SHE_KEY_STORE_COUNTER SHE_FEATURE_NOT_SUPPORTED SHE_KEY_STORE_CONFLICT SHE_FEATURE_NOT_SUPPORTED SHE_KEY_STORE_COUNTER SHE_FEATURE_NOT_SUPPORTED SHE_SELF_TEST_FAILURE SHE_NOT_READY System not ready to accept service request. SHE_NOT_READY SHE_NOT_READY SHE_NOT_AVAILABLE_RATING SHE_KEY_NOT_AVAILABLE_RATING SHE_KEY_NOT_AVAILABLE_RATING SHE_KEY_NOT_AVAILABLE_RATING SHE_KEY_NOT_AVAILABLE_RATING SHE_KEY_NOT_RATING SHE_KEY_UPDATE_EROR_RATING SHE_KEY_UPDATE_EROR_RATING SHE_KEY_UPDATE_EROR_RATING SHE_KEY_UPDATE_EROR_RATING SHE_KEY_UPDATE_EROR_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_ERROR_SATING SHE_KEY_UPDATE_ERROR_SATING SHE_	SHE_INVALID_MESSAGE	Invalid/Unknown message.
SHE_INVALID_PARAM SHE_NVM_ERRO NVM general error. SHE_OUT_OF_MEMORY SHE_UNKNOWN_HANDLE SHE_UNKNOWN_KEY_STORE SHE_UNKNOWN_KEY_STORE SHE_UNKNOWN_KEY_STORE SHE_KEY_STORE_AUTH SHE_KEY_STORE_AUTH SHE_KEY_STORE_AUTH A key store authentication is failing. SHE_KEY_STORE_AUTH SHE_INC_CONFLICT SHE_ID_CONFLICT A Key store using the same key id already exists (create operation). SHE_RNG_NOT_STARTED Internal RNG not started. SHE_CMD_NOT_SUPPORTED Functionality not supported on current service configuration. SHE_KEY_STORE_CONFLICT SHE_KEY_STORE_CONFLICT SHE_KEY_STORE_CONFLICT SHE_KEY_STORE_CONFLICT SHE_KEY_STORE_CONFLICT SHE_KEY_STORE_OUNTER SHE_FEATURE_NOT_SUPPORTED Feature is not supported. SHE_SELF_TEST_FAILURE SHE_SELF_TEST_FAILURE SHE_SELF_TEST_FAILURE SHE_SELF_TEST_FAILURE SHE_SELF_TEST_FAILURE SHE_SELF_TEST_FAILURE SHE_SELF_TEST_FAILURE SHE_SEQUENCE_ERROR_RATING Invalid sequence of commands. SHE_KEY_INVALID_RATING SHE_KEY_INVALID_RATING SHE_KEY_LEMPTY_RATING SHE_KEY_UPDATE_BRATING SHE_KEY_UPDATE_BRATING SHE_KEY_UPDATE_BRATING SHE_KEY_UPDATE_ERROR_RATING SHE_NO_DEBUGGING_RATING SHE_NO_DEBUGGING_RATING SHE_NO_DEBUGGING_RATING SHE_MEMORY_FAILURE_RATING SHE_BUSY_RATING SHE_BUSY_RATING SHE_BUSY_RATING SHE is busy. SHE_MEMORY_FAILURE_RATING SHE SHE_IBBRY_RATING SHE ShE_SHEROR_RATING SHE ShE_BUSY_RATING SHE ShE_SHEROR_RATING SHE ShE_BUSY_RATING SHE ShE_SHEROR_RATING SHE ShE_BUSY_RATING SHE ShE_SHEROR_RATING SHE ShE_SHEROR_RATING SHE ShE_BUSY_RATING SHE ShE_SHEROR_RATING SHE ShE_SHEROR_RATING SHE ShE_SHEROR_RATING SHE ShE_SHEROR_RATING SHE ShE_SHEROR_RATING SHE ShE_SHEROR_RATING SHE SHE_SHEROR_SHATING SHE SHE_SHEROR_SHATING SHE SHE SHEROR_SHATING SHE SHE SHE SHEROR		Invalid Address.
SHE_NVM_ERRO SHE_UNKNOWN_HANDLE SHE_UNKNOWN_HANDLE SHE_UNKNOWN_KEY_STORE SHE_UNKNOWN_KEY_STORE SHE_UNKNOWN_KEY_STORE SHE_KEY_STORE_AUTH A key store with provided key store ID does not exist (load operation). SHE_KEY_STORE_AUTH A key store creation/load failure. SHE_ID_CONFLICT A key store using the same key id already exists (create operation). SHE_RNG_NOT_STARTED Internal RNG not started. SHE_OMD_NOT_SUPPORTED Functionality not supported on current service configuration. SHE_INVALID_LIFECYCLE Invalid lifecycle for requested operation. SHE_KEY_STORE_CONFLICT The key store already exists (load operation). SHE_KEY_STORE_COUNTER SHE_FEATURE_NOT_SUPPORTED Feature is not supported. SHE_SELF_TEST_FAILURE SHE_NOT_READY System not ready to accept service request. Feature disabled. SHE_UNKNOWN_WARNING SHE_UNKNOWN_WARNING SHE_UNKNOWN_WARNING SHE_UNKNOWN_WARNING SHE_KEY_NOT_AVAILABLE_RATING Invalid sequence of commands. SHE_KEY_EMPTY_RATING Key is locked. SHE_KEY_EMPTY_RATING Key has not been initialized yet. SHE_KEY_EMPTY_RATING SHE_KEY_WRITE_PROTECTED_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_MOD_SECURE_BOOT_FATING SHE_MOD_SECURE_BOOT_FATING Internal debugging is not possible. SHE_NO_SECURE_BOOT_SATING SHE_BUSY_RATING SHE is busy. SHE_MEMORY_FAILURE_RATING Memory Error. SHE_IBERROR SHE IBERROR SHE IBERROR SHE IBERROR SHE IBERROR SHE IBERROR. SHE IBERROR SHE IBERROR SHE IBERROR. SHE IBERROR S		Unknown ld.
SHE_OUT_OF_MEMORY SHE_UNKNOWN_HANDLE Unknown handle. SHE_UNKNOWN_KEY_STORE Key store with provided key store ID does not exist (load operation). SHE_KEY_STORE_AUTH A key store authentication is failing. SHE_KEY_STORAGE_ERROR Key store creation/load failure. SHE_ID_CONFLICT A Key store using the same key id already exists (create operation). SHE_RNG_NOT_STARTED Internal RNG not started. SHE_CMD_NOT_SUPPORTED Functionality not supported on current service configuration. SHE_INVALID_LIFECYCLE Invalid lifecycle for requested operation. SHE_KEY_STORE_CONFLICT The key store already exists (load operation). SHE_KEY_STORE_COUNTER Issue occurred while updating the key store counter. SHE_FEATURE_NOT_SUPPORTED Feature is not supported. SHE_SELF_TEST_FAILURE Self test execution failed. SHE_NOT_READY System not ready to accept service request. SHE_FEATURE_DISABLED Feature disabled. SHE_UNKNOWN_WARNING SHE_UNKNOWN_WARNING SHE_UNKNOWN_WARNING SHE_UNKNOWN_WARNING SHE_KEY_NOT_AVAILABLE_RATING Invalid sequence of commands. SHE_KEY_NOT_AVAILABLE_RATING Key is locked. SHE_KEY_EMPTY_RATING SHE_NO_SECURE_BOOT_RATING Conditions for a secure boot process are not met. SHE_KEY_WRITE_PROTECTED_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_NO_DEBUGGING_RATING Internal debugging is not possible. SHE_NO_DEBUGGING_RATING SHE_BUSY_RATING SHE is busy. SHE_MEMORY_FAILURE_RATING Memory Error. SHE_IB_ERROR SHE library error.	SHE_INVALID_PARAM	
SHE_UNKNOWN_HANDLE SHE_UNKNOWN_KEY_STORE SHE_UNKNOWN_KEY_STORE SHE_KEY_STORE_AUTH A key store authentication is failing. SHE_KEY_STORAGE_ERROR SHE_KEY_STORAGE_ERROR SHE_KEY_STORAGE_ERROR SHE_ID_CONFLICT A key store creation/load failure. A key store using the same key id already exists (create operation). SHE_RNG_NOT_STARTED Internal RNG not started. SHE_CMD_NOT_SUPPORTED Functionality not supported on current service configuration. SHE_KEY_STORE_CONFLICT The key store already exists (load operation). SHE_KEY_STORE_CONFLICT The key store already exists (load operation). SHE_KEY_STORE_COUNTER Issue occurred while updating the key store counter. SHE_FEATURE_NOT_SUPPORTED SHE_SELF_TEST_FAILURE Self test execution failed. SHE_NOT_READY System not ready to accept service request. SHE_FEATURE_DISABLED Feature disabled. SHE_UNKNOWN_WARNING SHE_UNKNOWN_WARNING SHE_KEY_NOT_AVAILABLE_RATING Key is locked. SHE_KEY_INVALID_RATING SHE_KEY_INVALID_RATING Key has not been initialized yet. SHE_NO_SECURE_BOOT_RATING Conditions for a secure boot process are not met. SHE_KEY_WRITE_PROTECTED_RATING Memory slot for this key has been write-protected. SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_BUSY_RATING SHE is busy. SHE_MEMORY_FAILURE_RATING SHE General error. SHE_MEMORY_FAILURE_RATING SHE General error.		NVM general error.
SHE_UNKNOWN_KEY_STORE SHE_KEY_STORE_AUTH SHE_KEY_STORE_AUTH SHE_KEY_STORE_AUTH SHE_KEY_STORE_AUTH SHE_KEY_STORE_AUTH A key store authentication is failing. SHE_ID_CONFLICT A key store creation/load failure. SHE_ID_CONFLICT A key store using the same key id already exists (create operation). SHE_RNG_NOT_STARTED Internal RNG not started. SHE_CMD_NOT_SUPPORTED Functionality not supported on current service configuration. SHE_INVALID_LIFECYCLE Invalid_lifecycle for requested operation. SHE_KEY_STORE_CONFLICT SHE_KEY_STORE_COUNTER Issue occurred while updating the key store counter. SHE_FEATURE_NOT_SUPPORTED Feature is not supported. SHE_SELF_TEST_FAILURE Self test execution failed. SHE_NOT_READY System not ready to accept service request. SHE_FEATURE_DISABLED Feature disabled. SHE_UNKNOWN_WARNING SHE_UNKNOWN_WARNING SHE_SEQUENCE_ERROR_RATING Invalid sequence of commands. SHE_KEY_NOT_AVAILABLE_RATING Key is locked. SHE_KEY_INVALID_RATING Key has not been initialized yet. SHE_NO_SECURE_BOOT_RATING SHE_KEY_WRITE_PROTECTED_RATING SHE_KEY_WRITE_PROTECTED_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_RNG_SEED_RATING SHE_BUSY_RATING SHE is busy. SHE_MEMORY_FAILURE_RATING SHE is busy. SHE_MEMORY_FAILURE_RATING SHE_GENERAL_ERROR SHE_BIBARCAR		Internal memory allocation failed.
operation). SHE_KEY_STORE_AUTH A key store authentication is failing. SHE_KEY_STORAGE_ERROR Key store creation/load failure. SHE_ID_CONFLICT A Key store using the same key id already exists (create operation). SHE_RNG_NOT_STARTED Internal RNG not started. SHE_CMD_NOT_SUPPORTED Functionality not supported on current service configuration. SHE_INVALID_LIFECYCLE Invalid lifecycle for requested operation. SHE_KEY_STORE_CONFLICT The key store already exists (load operation). SHE_KEY_STORE_COUNTER Issue occurred while updating the key store counter. SHE_FEATURE_NOT_SUPPORTED Feature is not supported. SHE_SELF_TEST_FAILURE Self test execution failed. SHE_NOT_SEADY System not ready to accept service request. SHE_FEATURE_DISABLED Feature disabled. SHE_UNKNOWN_WARNING SHE Unknown Warning. SHE_SEQUENCE_ERROR_RATING Invalid sequence of commands. SHE_KEY_INOT_AVAILABLE_RATING Key is locked. SHE_KEY_INVALID_RATING Key not allowed for the given operation. SHE_KEY_EMPTY_RATING Key has not been initialized yet. SHE_NO_SECURE_BOOT_RATING Conditions for a secure boot process are not met. SHE_KEY_WRITE_PROTECTED_RATING Key update did not succeed, errors in verification of message. SHE_KEY_UPDATE_ERROR_RATING Internal debugging is not possible. SHE_BUSY_RATING SHE is busy. SHE_MEMORY_FAILURE_RATING Memory Error. SHE_LIB_ERROR SHE library error.		
SHE_KEY_STORAGE_ERROR SHE_ID_CONFLICT SHE_ID_CONFLICT A Key store using the same key id already exists (create operation). SHE_RNG_NOT_STARTED Internal RNG not started. SHE_OMD_NOT_SUPPORTED SHE_INVALID_LIFECYCLE Invalid lifecycle for requested operation. SHE_KEY_STORE_CONFLICT SHE_KEY_STORE_COUNTER SHE_FEATURE_NOT_SUPPORTED SHE_FEATURE_NOT_SUPPORTED SHE_SELF_TEST_FAILURE SHE_NOT_READY SHE_NOT_READY SHE_NOT_READY SHE_NOT_READY SHE_UNKNOWN_WARNING SHE_SEQUENCE_ERROR_RATING SHE_KEY_INVALID_RATING SHE_KEY_INVALID_RATING SHE_KEY_EMPTY_RATING SHE_NO_SECURE_BOOT_RATING SHE_NO_SECURE_BOOT_RATING SHE_KEY_WRITE_PROTECTED_RATING SHE_REY_UPDATE_ERROR_RATING SHE_NO_DEBUGGING_RATING SHE_NO_DEBUGGING_RATING SHE_BUSY_RATING SHE_BUSY_RATING SHE_BUSY_RATING SHE_GENERAL_ERROR SHE_GENERAL_ERROR SHE_GENERAL_ERROR SHE_GENERAL_ERROR SHE library error.	SHE_UNKNOWN_KEY_STORE	
SHE_ID_CONFLICT A Key store using the same key id already exists (create operation). SHE_RNG_NOT_STARTED SHE_CMD_NOT_SUPPORTED SHE_INVALID_LIFECYCLE SHE_KEY_STORE_CONFLICT SHE_KEY_STORE_CONFLICT SHE_KEY_STORE_COUNTER SHE_FEATURE_NOT_SUPPORTED SHE_FEATURE_NOT_SUPPORTED SHE_SELF_TEST_FAILURE SHE_NOT_READY SHE_NOT_READY SHE_UNKNOWN_WARNING SHE_SEQUENCE_ERROR_RATING SHE_KEY_INVALID_RATING SHE_KEY_INVALID_RATING SHE_KEY_NOT_AVAILABLE_RATING SHE_KEY_EMPTY_RATING SHE_KEY_WRITE_PROTECTED_RATING SHE_KEY_WRITE_PROTECTED_RATING SHE_KEY_WRITE_PROTECTED_RATING SHE_REY_UNDTESTED SHE_RNG_SEED_RATING SHE_NO_DEBUGGING_RATING SHE_NO_DEBUGGING_RATING SHE_MEMORY_FAILURE_RATING SHE_MEMORY_FAILURE_RATING SHE_MEMORY_FAILURE_RATING SHE_MEMORY_FAILURE_RATING SHE_MEMORY_FAILURE_RATING SHE_MEMORY_FAILURE_RATING SHE_MEMORY_FAILURE_RATING SHE_GENERAL_ERROR SHE_GENERAL_ERROR SHE General error. SHE_IBLBERROR SHE General error.	SHE_KEY_STORE_AUTH	A key store authentication is failing.
operation). SHE_RNG_NOT_STARTED Internal RNG not started. SHE_CMD_NOT_SUPPORTED Functionality not supported on current service configuration. SHE_INVALID_LIFECYCLE Invalid lifecycle for requested operation. SHE_KEY_STORE_CONFLICT The key store already exists (load operation). SHE_KEY_STORE_COUNTER Issue occurred while updating the key store counter. SHE_FEATURE_NOT_SUPPORTED Feature is not supported. SHE_NOT_READY System not ready to accept service request. SHE_NOT_ISABLED Feature disabled. SHE_UNKNOWN_WARNING SHE Unknown Warning. SHE_SEQUENCE_ERROR_RATING Invalid sequence of commands. SHE_KEY_NOT_AVAILABLE_RATING Key is locked. SHE_KEY_INVALID_RATING Key not allowed for the given operation. SHE_KEY_EMPTY_RATING Conditions for a secure boot process are not met. SHE_KEY_WRITE_PROTECTED_RATING Memory slot for this key has been write-protected. SHE_RY_UPDATE_ERROR_RATING Key update did not succeed, errors in verification of message. SHE_NO_DEBUGGING_RATING Internal debugging is not possible. SHE_BUSY_RATING SHE is busy. SHE_MEMORY_FAILURE_RATING Memory Error. SHE_LIB_ERROR SHE library error.	SHE_KEY_STORAGE_ERROR	Key store creation/load failure.
SHE_CMD_NOT_SUPPORTED SHE_INVALID_LIFECYCLE SHE_KEY_STORE_CONFLICT SHE_KEY_STORE_CONFLICT SHE_KEY_STORE_COUNTER SHE_KEY_STORE_COUNTER SHE_FEATURE_NOT_SUPPORTED SHE_SELF_TEST_FAILURE SHE_NOT_READY SHE_FEATURE_DISABLED SHE_UNKNOWN_WARNING SHE_SEQUENCE_ERROR_RATING SHE_KEY_INVALID_RATING SHE_KEY_EMPTY_RATING SHE_KEY_WRITE_PROTECTED_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_NO_DEBUGGING_RATING SHE_NO_DEBUGGING_RATING SHE_NO_DEBUGGING_RATING SHE_BUSY_RATING SHE_BUSY_RATING SHE_MEMORY_FAILURE_RATING SHE_MEMORY_FAILURE_RATING SHE_MEMORY_FAILURE_RATING SHE_MEMORY_FAILURE_RATING SHE_BUSY_RATING SHE_GENERAL_ERROR SHE General error. SHE_LIB_ERROR SHE General error.	SHE_ID_CONFLICT	
SHE_INVALID_LIFECYCLE SHE_KEY_STORE_CONFLICT SHE_KEY_STORE_CONFLICT SHE_KEY_STORE_COUNTER SHE_KEY_STORE_COUNTER Issue occurred while updating the key store counter. SHE_FEATURE_NOT_SUPPORTED Feature is not supported. SHE_SELF_TEST_FAILURE SHE_NOT_READY System not ready to accept service request. Feature disabled. SHE_UNKNOWN_WARNING SHE_UNKNOWN_WARNING SHE_SEQUENCE_ERROR_RATING Invalid sequence of commands. SHE_KEY_NOT_AVAILABLE_RATING SHE_KEY_INVALID_RATING SHE_KEY_EMPTY_RATING SHE_KEY_EMPTY_RATING SHE_KEY_WRITE_PROTECTED_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_NO_DEBUGGING_RATING SHE_NO_DEBUGGING_RATING SHE_NO_DEBUGGING_RATING SHE_BUSY_RATING SHE_BUSY_RATING SHE_BUSY_RATING SHE_BUSY_RATING SHE_BUSY_RATING SHE_BUSY_RATING SHE_GENERAL_ERROR SHE_BIB_ERROR	SHE_RNG_NOT_STARTED	Internal RNG not started.
SHE_KEY_STORE_CONFLICT SHE_KEY_STORE_COUNTER Issue occurred while updating the key store counter. SHE_FEATURE_NOT_SUPPORTED Feature is not supported. SHE_SELF_TEST_FAILURE Self test execution failed. SHE_NOT_READY System not ready to accept service request. Feature disabled. SHE_UNKNOWN_WARNING SHE_UNKNOWN_WARNING SHE_SEQUENCE_ERROR_RATING Invalid sequence of commands. SHE_KEY_NOT_AVAILABLE_RATING Key is locked. SHE_KEY_INVALID_RATING SHE_KEY_EMPTY_RATING Key has not been initialized yet. SHE_KEY_WRITE_PROTECTED_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_NO_SECURE_BOOT_RATING SHE_NO_DEBUGGING_RATING SHE_NO_DEBUGGING_RATING SHE_NO_DEBUGGING_RATING SHE_BUSY_RATING SHE_BUSY_RATING SHE_BUSY_RATING SHE_BUSY_RATING SHE_MEMORY_FAILURE_RATING SHE_GENERAL_ERROR SHE_Ibipary error.	SHE_CMD_NOT_SUPPORTED	Functionality not supported on current service configuration.
SHE_KEY_STORE_COUNTER	SHE_INVALID_LIFECYCLE	Invalid lifecycle for requested operation.
SHE_FEATURE_NOT_SUPPORTED SHE_SELF_TEST_FAILURE Self test execution failed. SHE_NOT_READY System not ready to accept service request. SHE_FEATURE_DISABLED Feature disabled. SHE_UNKNOWN_WARNING SHE_SEQUENCE_ERROR_RATING Invalid sequence of commands. SHE_KEY_NOT_AVAILABLE_RATING SHE_KEY_INVALID_RATING SHE_KEY_EMPTY_RATING SHE_KEY_EMPTY_RATING SHE_KEY_EMPTY_RATING SHE_KEY_WRITE_PROTECTED_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_REY_UPDATE_ERROR_RATING SHE_NO_DEBUGGING_RATING SHE_BUSY_RATING SHE_BUSY_RATING SHE_BUSY_RATING SHE_MEMORY_FAILURE_RATING SHE_GENERAL_ERROR SHE_GENERAL_ERROR SHE_GENERAL_ERROR SHE_BIDSY_BED_IND SHE_BURNOR SHE_BURNOR SHE_BURNOR SHE_BURNOR SHE_BURNOR SHE_GENERAL_ERROR SHE_BURNOR SH	SHE_KEY_STORE_CONFLICT	The key store already exists (load operation).
SHE_SELF_TEST_FAILURE Self test execution failed. SHE_NOT_READY System not ready to accept service request. SHE_FEATURE_DISABLED Feature disabled. SHE_UNKNOWN_WARNING SHE_Unknown Warning. SHE_SEQUENCE_ERROR_RATING Invalid sequence of commands. SHE_KEY_NOT_AVAILABLE_RATING Key is locked. SHE_KEY_INVALID_RATING Key not allowed for the given operation. SHE_KEY_EMPTY_RATING Key has not been initialized yet. SHE_NO_SECURE_BOOT_RATING Conditions for a secure boot process are not met. SHE_KEY_UPDATE_ERROR_RATING Key update did not succeed, errors in verification of message. SHE_RNG_SEED_RATING The seed has not been initialized. SHE_NO_DEBUGGING_RATING Internal debugging is not possible. SHE_BUSY_RATING SHE is busy. SHE_MEMORY_FAILURE_RATING Memory Error. SHE_GENERAL_ERROR SHE General error. SHE_LIB_ERROR SHE library error.	SHE_KEY_STORE_COUNTER	Issue occurred while updating the key store counter.
SHE_NO_SECURE_BRATING SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_KEY_UPDATE_RATING SHE_KEY_UPDATE_RATING SHE_REY_UPDATE_RATING SHE_BUSY_RATING SHE is busy. SHE_BUSY_RATING SHE is busy. SHE_MEMORY_FAILURE_RATING SHE General error. SHE_LIB_ERROR SHE library error.	SHE_FEATURE_NOT_SUPPORTED	Feature is not supported.
SHE_FEATURE_DISABLED Feature disabled. SHE_UNKNOWN_WARNING SHE Unknown Warning. SHE_SEQUENCE_ERROR_RATING Invalid sequence of commands. SHE_KEY_NOT_AVAILABLE_RATING Key is locked. SHE_KEY_INVALID_RATING Key not allowed for the given operation. SHE_KEY_EMPTY_RATING Key has not been initialized yet. SHE_NO_SECURE_BOOT_RATING Conditions for a secure boot process are not met. SHE_KEY_WRITE_PROTECTED_RATING Memory slot for this key has been write-protected. SHE_KEY_UPDATE_ERROR_RATING Key update did not succeed, errors in verification of message. SHE_RNG_SEED_RATING The seed has not been initialized. SHE_NO_DEBUGGING_RATING Internal debugging is not possible. SHE_BUSY_RATING SHE is busy. SHE_MEMORY_FAILURE_RATING Memory Error. SHE_LIB_ERROR SHE General error. SHE_LIB_ERROR SHE library error.	SHE_SELF_TEST_FAILURE	Self test execution failed.
SHE_UNKNOWN_WARNING SHE_SEQUENCE_ERROR_RATING Invalid sequence of commands. SHE_KEY_NOT_AVAILABLE_RATING SHE_KEY_INVALID_RATING SHE_KEY_EMPTY_RATING SHE_KEY_EMPTY_RATING SHE_NO_SECURE_BOOT_RATING SHE_KEY_WRITE_PROTECTED_RATING SHE_KEY_UPDATE_ERROR_RATING SHE_RNG_SEED_RATING SHE_NO_DEBUGGING_RATING SHE_NO_DEBUGGING_RATING SHE_BUSY_RATING SHE_BUSY_RATING SHE_BUSY_RATING SHE_BUSY_RATING SHE_GENERAL_ERROR SHE_GENERAL_ERROR SHE_IDDATE_ERROR SHE_BUSY_ERROR SHE_GENERAL_ERROR SHE_BUSY_ERROR SHE_GENERAL_ERROR SHE_IDDATE_ERROR SHE_IDDATE_ERROR SHE_GENERAL_ERROR SHE_IDDATE_ERROR SHE_GENERAL_ERROR SHE_GENERAL_ERROR SHE_IDDATE SHE_	SHE_NOT_READY	
SHE_SEQUENCE_ERROR_RATING Invalid sequence of commands. SHE_KEY_NOT_AVAILABLE_RATING Key is locked. SHE_KEY_INVALID_RATING Key not allowed for the given operation. SHE_KEY_EMPTY_RATING Key has not been initialized yet. SHE_NO_SECURE_BOOT_RATING Conditions for a secure boot process are not met. SHE_KEY_WRITE_PROTECTED_RATING Memory slot for this key has been write-protected. SHE_KEY_UPDATE_ERROR_RATING Key update did not succeed, errors in verification of message. SHE_RNG_SEED_RATING The seed has not been initialized. SHE_NO_DEBUGGING_RATING Internal debugging is not possible. SHE_BUSY_RATING SHE is busy. SHE_MEMORY_FAILURE_RATING Memory Error. SHE_GENERAL_ERROR SHE General error. SHE_LIB_ERROR SHE library error.		
SHE_KEY_NOT_AVAILABLE_RATING Key is locked. SHE_KEY_INVALID_RATING Key not allowed for the given operation. SHE_KEY_EMPTY_RATING Key has not been initialized yet. SHE_NO_SECURE_BOOT_RATING Conditions for a secure boot process are not met. SHE_KEY_WRITE_PROTECTED_RATING Memory slot for this key has been write-protected. SHE_KEY_UPDATE_ERROR_RATING Key update did not succeed, errors in verification of message. SHE_RNG_SEED_RATING The seed has not been initialized. SHE_NO_DEBUGGING_RATING Internal debugging is not possible. SHE_BUSY_RATING SHE is busy. SHE_MEMORY_FAILURE_RATING Memory Error. SHE_GENERAL_ERROR SHE General error. SHE_LIB_ERROR SHE library error.		-
SHE_KEY_INVALID_RATING Key not allowed for the given operation. SHE_KEY_EMPTY_RATING Key has not been initialized yet. SHE_NO_SECURE_BOOT_RATING Conditions for a secure boot process are not met. SHE_KEY_WRITE_PROTECTED_RATING Memory slot for this key has been write-protected. SHE_KEY_UPDATE_ERROR_RATING Key update did not succeed, errors in verification of message. SHE_RNG_SEED_RATING The seed has not been initialized. SHE_NO_DEBUGGING_RATING Internal debugging is not possible. SHE_BUSY_RATING SHE is busy. SHE_MEMORY_FAILURE_RATING Memory Error. SHE_GENERAL_ERROR SHE General error. SHE_LIB_ERROR SHE library error.		•
SHE_KEY_EMPTY_RATING Key has not been initialized yet. SHE_NO_SECURE_BOOT_RATING Conditions for a secure boot process are not met. SHE_KEY_WRITE_PROTECTED_RATING Memory slot for this key has been write-protected. SHE_KEY_UPDATE_ERROR_RATING Key update did not succeed, errors in verification of message. SHE_RNG_SEED_RATING The seed has not been initialized. SHE_NO_DEBUGGING_RATING Internal debugging is not possible. SHE_BUSY_RATING SHE is busy. SHE_MEMORY_FAILURE_RATING Memory Error. SHE_GENERAL_ERROR SHE General error. SHE_LIB_ERROR SHE library error.	SHE_KEY_NOT_AVAILABLE_RATING	Key is locked.
SHE_NO_SECURE_BOOT_RATING Conditions for a secure boot process are not met. SHE_KEY_WRITE_PROTECTED_RATING Memory slot for this key has been write-protected. SHE_KEY_UPDATE_ERROR_RATING Key update did not succeed, errors in verification of message. SHE_RNG_SEED_RATING The seed has not been initialized. SHE_NO_DEBUGGING_RATING Internal debugging is not possible. SHE_BUSY_RATING SHE is busy. SHE_MEMORY_FAILURE_RATING Memory Error. SHE_GENERAL_ERROR SHE General error. SHE_LIB_ERROR SHE library error.	SHE_KEY_INVALID_RATING	Key not allowed for the given operation.
SHE_KEY_WRITE_PROTECTED_RATING Memory slot for this key has been write-protected. SHE_KEY_UPDATE_ERROR_RATING Key update did not succeed, errors in verification of message. SHE_RNG_SEED_RATING The seed has not been initialized. SHE_NO_DEBUGGING_RATING Internal debugging is not possible. SHE_BUSY_RATING SHE is busy. SHE_MEMORY_FAILURE_RATING Memory Error. SHE_GENERAL_ERROR SHE General error. SHE_LIB_ERROR SHE library error.	SHE_KEY_EMPTY_RATING	Key has not been initialized yet.
SHE_KEY_UPDATE_ERROR_RATING Key update did not succeed, errors in verification of message. SHE_RNG_SEED_RATING The seed has not been initialized. SHE_NO_DEBUGGING_RATING Internal debugging is not possible. SHE_BUSY_RATING SHE is busy. SHE_MEMORY_FAILURE_RATING Memory Error. SHE_GENERAL_ERROR SHE General error. SHE_LIB_ERROR SHE library error.		Conditions for a secure boot process are not met.
SHE_RNG_SEED_RATING The seed has not been initialized. SHE_NO_DEBUGGING_RATING Internal debugging is not possible. SHE_BUSY_RATING SHE is busy. SHE_MEMORY_FAILURE_RATING Memory Error. SHE_GENERAL_ERROR SHE General error. SHE_LIB_ERROR SHE library error.		· · · · · · · · · · · · · · · · · · ·
SHE_NO_DEBUGGING_RATING Internal debugging is not possible. SHE_BUSY_RATING SHE is busy. SHE_MEMORY_FAILURE_RATING Memory Error. SHE_GENERAL_ERROR SHE General error. SHE_LIB_ERROR SHE library error.	SHE_KEY_UPDATE_ERROR_RATING	Key update did not succeed, errors in verification of message.
SHE_BUSY_RATING SHE is busy. SHE_MEMORY_FAILURE_RATING Memory Error. SHE_GENERAL_ERROR SHE General error. SHE_LIB_ERROR SHE library error.		
SHE_MEMORY_FAILURE_RATING Memory Error. SHE_GENERAL_ERROR SHE General error. SHE_LIB_ERROR SHE library error.		35 5 .
SHE_GENERAL_ERROR SHE General error. SHE_LIB_ERROR SHE library error.		-
SHE_LIB_ERROR SHE library error.		-
SHE FATAL FAILURE fatal error		-
GITE_INTRESITE INCOME	SHE_FATAL_FAILURE	fatal error

5.18 Utils 39

5.18 Utils

User must open a SHE utils service flow in order to perform the following operations:

Data Structures

· struct op_open_utils_args_t

Functions

- she_err_t she_open_utils (she_hdl_t key_store_handle, op_open_utils_args_t *args)
- she_err_t she_close_utils (she_hdl_t utils_handle)

5.18.1 Detailed Description

User must open a SHE utils service flow in order to perform the following operations:

- · Create a utils handle
- · perform SHE key update extension
- · update SHE plain key
- · export SHE plain key
- get SHE identity (UID)
- · get SHE status register
- perform MAC generation and verification in fast mode for a SHE session on V2X
- perform MAC generation and verification in fast mode for a SHE session

5.18.2 Data Structure Documentation

5.18.2.1 struct op_open_utils_args_t Structure describing the open utils service operation arguments

Data Fields

```
uint32_t utils_handle
```

5.18.3 Function Documentation

Open SHE utils service flow on the specified key store. The SHE utils service flow can be opened only after opening SHE key storage handle.

5.18 Utils 41

Parameters

key_store_handle	handle identifying the key store service.
args	pointer to the structure containing the function arguments.

Returns

error code.

Terminate a previously opened utils service flow

Parameters

	utils_handle	handle identifying the utils service.
--	--------------	---------------------------------------

Returns

error code.

5.19 last rating code

Functions

• uint32_t she_get_last_rating_code (she_hdl_t session_hdl)

5.19.1 Detailed Description

5.19.2 Function Documentation

Report rating code from last command

SHE API defines standard errors that should be returned by API calls. Error code reported by SECO are "translated" to these SHE error codes. This API allow user to get the error code reported by SECO for the last command before its translation to SHE error codes. This should be used for debug purpose only.

Parameters

session_hdl	SHE session handler
-------------	---------------------

Returns

rating code reported by last command

5.20 CMD_CANCEL 43

5.20 CMD_CANCEL

Functions

void she_cmd_cancel (void)

5.20.1 Detailed Description

5.20.2 Function Documentation

5.20.2.1 she_cmd_cancel() void she_cmd_cancel (
$$void$$
)

interrupt any given function and discard all calculations and results.

5.21 Get Info

Data Structures

• struct op_get_info_args_t

5.21.1 Detailed Description

5.21.2 Data Structure Documentation

5.21.2.1 struct op_get_info_args_t Structure describing the get info operation member arguments

Data Fields

uint32_t	user_sab_id	Stores User identifier (32bits)
uint8_t *	chip_unique_id	Stores the chip unique identifier.
uint16_t	chip_unq_id_sz	Size of the chip unique identifier in bytes.
uint16_t	chip_monotonic_counter	Stores the chip monotonic counter value (16bits)
uint16_t	chip_life_cycle	Stores the chip current life cycle bitfield (16bits)
uint32_t	version	Stores the module version (32bits)
uint32_t	version_ext	Stores the module extended version (32bits)
uint8_t	fips_mode	Stores the FIPS mode bitfield (8bits). Bitmask definition: bit0 - FIPS mode of operation:
		value 0 - part is running in FIPS non-approved mode.
		 value 1 - part is running in FIPS approved mode. bit1 - FIPS certified part:
		value 0 - part is not FIPS certified.
		value 1 - part is FIPS certified. bit2-7: reserved
		• value 0.

5.22 Global Info 45

5.22 Global Info

Macros

- #define SOC_IMX8DXL 0xe
- #define SOC IMX8ULP 0x84d
- #define **SOC_IMX93** 0x9300
- #define SOC_IMX95 0x9500
- #define SOC_REV_A0 0xa000
- #define SOC_REV_A1 0xa100
- #define SOC REV A2 0xa200
- #define SOC_REV_B0 0xb000
- #define SOC LF FAB DEFAULT 0x1
- #define SOC LF FAB MODE 0x2
- #define SOC_LF_NO_NXP_SECRETS 0x4
- #define SOC LF WITH NXP SECRETS 0x8
- #define SOC LF SCU FW CLOSED 0x10
- #define SOC_LF_SECO_FW_CLOSED 0x20
- #define SOC_LF_CLOSED 0x40
- #define SOC_LF_CLOSED_WITH_NXP_FW 0x80
- #define SOC_LF_PARTIAL_FIELD_RET 0x100
- #define SOC LF_FIELD_RET 0x200
- #define SOC_LF_NO_RET 0x400
- #define GINFO_LIB_VERSION_LEN 16
- #define GINFO_NVM_VERSION_LEN 16
- #define GINFO COMMIT ID SZ 40
- #define HSM_API_VERSION_1 0x1
- #define HSM API VERSION 2 0x2

Functions

- · void populate global info (uint32 t session hdl)
- void show_global_info (void)
- bool is_global_info_populated (void)
- uint16 t se get soc id (void)
- uint16_t se_get_soc_rev (void)
- uint16_t se_get_chip_lifecycle (void)
- uint8_t se_get_fips_mode (void)
- uint8_t se_get_lib_newness_ver (void)
- uint8_t se_get_lib_major_ver (void)
- uint8_t se_get_lib_minor_ver (void)
- uint8_t se_get_nvm_newness_ver (void)
- uint8_t se_get_nvm_major_ver (void)
- uint8_t se_get_nvm_minor_ver (void)
- const char * se_get_commit_id (void)
- const char * se_get_lib_version (void)
- const char * se_get_nvm_version (void)
- const char * get_soc_id_str (uint16_t soc_id)
- const char * get_soc_rev_str (uint16_t soc_rev)
- const char * get_soc_lf_str (uint16_t lifecycle)
- void se_get_info (uint32_t session_hdl, op_get_info_args_t *args)
- void se_get_soc_info (uint32_t session_hdl, uint16_t *soc_id, uint16_t *soc_rev)

5.22.1 Detailed Description

5.22.2 Function Documentation

```
5.22.2.1 populate_global_info() void populate_global_info ( uint32_t session_hdl )
```

Populate the Global Info structure

Parameters

```
session_hdl identifying the session.
```

Print the Global Info of library

Get the status of Global Info, if populated or not.

```
5.22.2.4 se_get_soc_id() uint16_t se_get_soc_id ( void )
```

Get SoC ID.

5.22.2.5 se_get_soc_rev() uint16_t se_get_soc_rev (
$$void$$
)

Get SoC Revision.

Get Chip-lifecycle.

Get Fips mode.

5.22 Global Info 47

```
5.22.2.8 se_get_lib_newness_ver() uint8_t se_get_lib_newness_ver ( void )
```

Get library newness version.

Get library major version.

Get library minor version.

Get NVM newness version.

Get NVM major version.

Get NVM minor version.

5.22.2.14 se_get_commit_id() const char* se_get_commit_id (
$$void$$
)

Get Build commit id.

Get library version string.

Get NVM version string.

Get the string representating SoC ID

Parameters

soc⊷	SoC ID fetched from Global Info
_id	

Returns

String represention of the SoC ID

```
5.22.2.18 get_soc_rev_str() const char* get_soc_rev_str ( uint16_t soc_rev )
```

Get the string representating SoC Revision

Parameters

Returns

String represention of the SoC Revision

```
5.22.2.19 get_soc_lf_str() const char* get_soc_lf_str ( uint16_t lifecycle )
```

Get the string representation of the Chip Lifecycle

Parameters

1	life evele	value fetales d'franc Clabal Info
	illecycle	value fetched from Global Info

Returns

a string represention of Lifecycle

Get Info for Global Info setup

5.22 Global Info 49

Get SoC Info for Global Info setup

Index

add_she_service	SHE_INVALID_LIFECYCLE, 38
Session, 20	SHE_INVALID_MESSAGE, 38
add_she_session	SHE_INVALID_PARAM, 38
Session, 20	SHE_KEY_EMPTY_RATING, 38
	SHE_KEY_INVALID_RATING, 38
CMD_CANCEL, 43	SHE_KEY_NOT_AVAILABLE_RATING, 38
she_cmd_cancel, 43	SHE_KEY_STORAGE_ERROR, 38
CMD_ENC_CBC / CMD_DEC_CBC and CMD_ENC_ECE	SHE_KEY_STORE_AUTH, 38
/ CMD_DEC_ECB, 2	SHE_KEY_STORE_CONFLICT, 38
she_cipher_one_go, 4	SHE_KEY_STORE_COUNTER, 38
SHE_CIPHER_ONE_GO_ALGO_AES_CCM, 3	SHE_KEY_UPDATE_ERROR_RATING, 38
SHE_CIPHER_ONE_GO_FLAGS_DECRYPT, 3	SHE_KEY_WRITE_PROTECTED_RATING, 38
SHE_CIPHER_ONE_GO_FLAGS_ENCRYPT, 3	SHE_LIB_ERROR, 38
she_close_cipher_service, 4	SHE_MEMORY_FAILURE_RATING, 38
she_op_cipher_one_go_algo_t, 3	SHE_NO_DEBUGGING_RATING, 38
she_op_cipher_one_go_flags_t, 3	SHE_NO_ERROR, 38
she_open_cipher_service, 3	SHE_NO_SECURE_BOOT_RATING, 38
CMD_EXPORT_RAM_KEY, 5	SHE_NOT_READY, 38
she_export_plain_key, 5	SHE NVM ERRO, 38
CMD_EXTEND_SEED, 33	SHE_OUT_OF_MEMORY, 38
SHE_ENTROPY_SIZE, 33	SHE_RNG_NOT_STARTED, 38
she_extend_seed, 33	SHE_RNG_SEED_RATING, 38
CMD_GENERATE_MAC, 9	SHE_SELF_TEST_FAILURE, 38
she_generate_mac, 10	SHE_SEQUENCE_ERROR_RATING, 38
she_get_id, 10	SHE UNKNOWN HANDLE, 38
CMD_GET_STATUS, 16	SHE_UNKNOWN_ID, 38
she_get_status, 16	SHE_UNKNOWN_KEY_STORE, 38
CMD_INIT_RNG, 30	SHE_UNKNOWN_WARNING, 38
she_close_rng_service, 30	/
she_open_rng_service, 30	FAST_MAC, 7
CMD_LOAD_KEY, 26	SHE_FAST_MAC_FLAGS_GENERATION, 8
she_key_update, 27	
she_key_update_ext, 27	Get Info, 44
CMD_LOAD_PLAIN_KEY, 29	get_soc_id_str
she_load_plain_key, 29	Global Info, 47
CMD_RND, 31	get_soc_lf_str
she_get_random, 32	Global Info, 48
SHE_RND_SIZE, 31	get_soc_rev_str
CMD_VERIFY_MAC, 11	Global Info, 48
she_verify_mac, 11	Global Info, 45
	get_soc_id_str, 47
delete_she_service	get_soc_lf_str, 48
Session, 20	get_soc_rev_str, 48
delete_she_session	is_global_info_populated, 46
Session, 19	populate_global_info, 46
	se_get_chip_lifecycle, 46
Error codes, 37	se_get_commit_id, 47
SHE_BUSY_RATING, 38	se_get_fips_mode, 46
SHE_CMD_NOT_SUPPORTED, 38	se_get_info, 48
she_err_t, 37	se_get_lib_major_ver, 47
SHE_FATAL_FAILURE, 38	se_get_lib_minor_ver, 47
SHE_FEATURE_DISABLED, 38	se_get_lib_newness_ver, 46
SHE_FEATURE_NOT_SUPPORTED, 38	se_get_lib_version, 47
SHE_GENERAL_ERROR, 38	se_get_nvm_major_ver, 47
SHE_ID_CONFLICT, 38	se_get_nvm_minor_ver, 47
SHE_INVALID_ADDRESS, 38	se_get_nvm_newness_ver, 47

52 INDEX

se_get_nvm_version, 47 se_get_soc_id, 46	open_svc_rng_args_t, 31
se_get_soc_info, 48	populate_global_info
se_get_soc_rev, 46	Global Info, 46
show_global_info, 46	
	se_get_chip_lifecycle
is_global_info_populated	Global Info, 46
Global Info, 46	se_get_commit_id
	Global Info, 47
Key store, 22	se_get_fips_mode
KEY_STORE_OPEN_FLAGS_CREATE, 24	Global Info, 46
KEY_STORE_OPEN_FLAGS_DEFAULT, 24	se_get_info
KEY_STORE_OPEN_FLAGS_SET_MAC_LEN, 24	
KEY_STORE_OPEN_FLAGS_SHARED, 24	se_get_lib_major_ver
KEY_STORE_OPEN_FLAGS_SHE, 24	Global Info, 47
KEY_STORE_OPEN_FLAGS_STRICT_OPERATION	
24	Global Info, 47
she_close_key_store_service, 25	se_get_lib_newness_ver
she_open_key_store_service, 24	Global Info, 46
SHE_STORAGE_MIN_MAC_BIT_LENGTH_DEFAL	
24	Global Info, 47
SHE_STORAGE_NUMBER_UPDATES_DEFAULT,	se_get_nvm_major_ver Global Info, 47
24	
KEY_STORE_OPEN_FLAGS_CREATE	se_get_nvm_minor_ver Global Info, 47
Key store, 24	se_get_nvm_newness_ver
KEY_STORE_OPEN_FLAGS_DEFAULT	Global Info, 47
Key store, 24	se_get_nvm_version
KEY_STORE_OPEN_FLAGS_SET_MAC_LEN	Global Info, 47
Key store, 24 KEY_STORE_OPEN_FLAGS_SHARED	se_get_soc_id
Key store, 24	Global Info, 46
KEY_STORE_OPEN_FLAGS_SHE	se_get_soc_info
Key store, 24	Global Info, 48
KEY_STORE_OPEN_FLAGS_STRICT_OPERATION	se get soc rev
Key store, 24	Global Info, 46
1.67 5.61.6, 2.7	Session, 17
last rating code, 42	add_she_service, 20
she_get_last_rating_code, 42	add_she_session, 20
	delete_she_service, 20
op_cipher_one_go_args_t, 35	delete_she_session, 19
op_export_plain_key_args_t, 5	she_close_session, 21
op_fast_seco_mac_t, 7	SHE_HANDLE_NONE, 18
op_fast_v2x_mac_t, 7	she_hdl_t, 19
op_generate_mac_t, 9	she_open_session, 21
op_get_id_args_t, 9	SHE_OPEN_SESSION_EXCLUSIVE_MASK, 18
op_get_info_args_t, 44	SHE_OPEN_SESSION_FIPS_MODE_MASK, 18
op_get_random_args_t, 31	SHE_OPEN_SESSION_LOW_LATENCY_MASK,
op_get_status_args_t, 16	18
op_key_store_reprov_en_args_t, 23	SHE_OPEN_SESSION_NO_KEY_STORE_MASK
op_key_update_args_t, 26	19
op_key_update_ext_args_t, 26	SHE_OPEN_SESSION_PRIORITY_HIGH, 18
op_load_plain_key_args_t, 29	SHE_OPEN_SESSION_PRIORITY_LOW, 18
op_open_utils_args_t, 39	she_service_hdl_to_ptr, 20
op_rng_extend_seed_t, 33	she_session_hdl_to_ptr, 19
op_shared_buf_args_t, 35	Shared Buffer, 35
op_verify_mac_t, 11	SHE got into 14
open_session_args_t, 18	SHE get info, 14
open_svc_cipher_args_t, 35 open_svc_key_store_args_t, 23	she_get_info, 14 SHE_BUSY_RATING
Upon 340 NEY SIDIE AIDS L. CU	OTIL DOOT HATING

INDEX 53

F d 00	OUE HANDLE MONE
Error codes, 38	SHE_HANDLE_NONE
she_cipher_one_go	Session, 18
CMD_ENC_CBC / CMD_DEC_CBC and CMD_ENC	_ El04B _hdl_t
/ CMD_DEC_ECB, 4	Session, 19
SHE_CIPHER_ONE_GO_ALGO_AES_CCM	SHE_ID_CONFLICT
CMD_ENC_CBC / CMD_DEC_CBC and CMD_ENC	ECB Error codes, 38
/ CMD_DEC_ECB, 3	SHE_INVALID_ADDRESS
SHE_CIPHER_ONE_GO_FLAGS_DECRYPT	Error codes, 38
CMD_ENC_CBC / CMD_DEC_CBC and CMD_ENC	
/ CMD_DEC_ECB, 3	Error codes, 38
SHE_CIPHER_ONE_GO_FLAGS_ENCRYPT	SHE_INVALID_MESSAGE
CMD_ENC_CBC / CMD_DEC_CBC and CMD_ENC	_ECB Error codes, 38
/ CMD_DEC_ECB, 3	SHE_INVALID_PARAM
she_close_cipher_service	Error codes, 38
CMD_ENC_CBC / CMD_DEC_CBC and CMD_ENC	SCHE KEY EMPTY RATING
/ CMD_DEC_ECB, 4	Error codes, 38
she_close_key_store_service	SHE_KEY_INVALID_RATING
Key store, 25	Error codes, 38
she_close_rng_service	SHE_KEY_NOT_AVAILABLE_RATING
CMD_INIT_RNG, 30	Error codes, 38
she_close_session	SHE_KEY_STORAGE_ERROR
Session, 21	Error codes, 38
she_close_utils	SHE_KEY_STORE_AUTH
Utils, 41	Error codes, 38
she_cmd_cancel	SHE_KEY_STORE_CONFLICT
CMD_CANCEL, 43	Error codes, 38
SHE_CMD_NOT_SUPPORTED	SHE_KEY_STORE_COUNTER
Error codes, 38	Error codes, 38
SHE_ENTROPY_SIZE	
	she_key_update
CMD_EXTEND_SEED, 33	CMD_LOAD_KEY, 27
she_err_t	SHE_KEY_UPDATE_ERROR_RATING
Error codes, 37	Error codes, 38
she_export_plain_key	she_key_update_ext
CMD_EXPORT_RAM_KEY, 5	CMD_LOAD_KEY, 27
she_extend_seed	SHE_KEY_WRITE_PROTECTED_RATING
CMD_EXTEND_SEED, 33	Error codes, 38
SHE FAST MAC FLAGS GENERATION	SHE_LIB_ERROR
FAST_MAC, 8	Error codes, 38
SHE FATAL FAILURE	she_load_plain_key
Error codes, 38	CMD_LOAD_PLAIN_KEY, 29
SHE_FEATURE_DISABLED	SHE_MEMORY_FAILURE_RATING
Error codes, 38	Error codes, 38
SHE_FEATURE_NOT_SUPPORTED	SHE_NO_DEBUGGING_RATING
Error codes, 38	Error codes, 38
SHE_GENERAL_ERROR	SHE_NO_ERROR
Error codes, 38	Error codes, 38
she_generate_mac	SHE_NO_SECURE_BOOT_RATING
CMD_GENERATE_MAC, 10	Error codes, 38
she_get_id	SHE_NOT_READY
CMD_GENERATE_MAC, 10	Error codes, 38
she_get_info	SHE_NVM_ERRO
SHE get info, 14	Error codes, 38
she_get_last_rating_code	she_op_cipher_one_go_algo_t
last rating code, 42	CMD_ENC_CBC / CMD_DEC_CBC and CMD_ENC_ECB
she_get_random	/ CMD_DEC_ECB, 3
CMD_RND, 32	she_op_cipher_one_go_flags_t
she_get_status	CMD_ENC_CBC / CMD_DEC_CBC and CMD_ENC_ECB
CMD GET STATUS, 16	/ CMD_DEC_ECB. 3

54 INDEX

```
she_open_cipher_service
                                                   she_close_utils, 41
    CMD_ENC_CBC / CMD_DEC_CBC and CMD_ENC_ECB she_open_utils, 39
        / CMD_DEC_ECB, 3
she_open_key_store_service
    Key store, 24
she open rng service
    CMD INIT RNG, 30
she_open_session
    Session, 21
SHE_OPEN_SESSION_EXCLUSIVE_MASK
    Session, 18
SHE_OPEN_SESSION_FIPS_MODE_MASK
    Session, 18
SHE_OPEN_SESSION_LOW_LATENCY_MASK
    Session, 18
SHE_OPEN_SESSION_NO_KEY_STORE_MASK
    Session, 19
SHE_OPEN_SESSION_PRIORITY_HIGH
    Session, 18
SHE_OPEN_SESSION_PRIORITY_LOW
    Session, 18
she open utils
    Utils, 39
SHE_OUT_OF_MEMORY
    Error codes, 38
SHE_RND_SIZE
    CMD_RND, 31
SHE RNG NOT STARTED
    Error codes, 38
SHE_RNG_SEED_RATING
    Error codes, 38
SHE_SELF_TEST_FAILURE
    Error codes, 38
SHE_SEQUENCE_ERROR_RATING
    Error codes, 38
she_service_hdl_s, 18
she_service_hdl_to_ptr
    Session, 20
she_session_hdl_s, 17
she session hdl to ptr
    Session, 19
SHE_STORAGE_MIN_MAC_BIT_LENGTH_DEFAULT
    Key store, 24
SHE STORAGE NUMBER UPDATES DEFAULT
    Key store, 24
SHE_UNKNOWN_HANDLE
    Error codes, 38
SHE UNKNOWN ID
    Error codes, 38
SHE_UNKNOWN_KEY_STORE
    Error codes, 38
SHE UNKNOWN WARNING
    Error codes, 38
she_verify_mac
    CMD_VERIFY_MAC, 11
show global info
    Global Info, 46
```

Utils, 39